10. BurpSuite - Fundamentals

🔍 Burp Suite

1. What is Burp Suite?

- Burp Suite is a comprehensive **web application security testing platform** widely used by penetration testers and security professionals.
- It acts as a **proxy**, intercepting and modifying HTTP/S traffic between your browser and the target web app.
- Provides tools for automated scanning, manual testing, attack simulation, and vulnerability analysis.

2. How Do You Set Up a Proxy in Burp Suite?

- Burp Suite acts as an **intercepting proxy** on a local port (default: 127.0.0.1:8080).
- To set up:
  1. Open Burp Suite and go to **Proxy > Options** to confirm proxy listener is active.
  2. Configure your browser to use **127.0.0.1:8080** as an HTTP/HTTPS proxy.
  3. Import Burp's CA certificate into your browser to intercept HTTPS without certificate errors.
  4. Once configured, all traffic flows through Burp for inspection and modification.

3. What Are Burp Suite's Main Components?

- **Proxy**: Intercepts, inspects, and modifies HTTP/S traffic.
- **Spider**: Crawls the target web app to map out pages, forms, and parameters.
- **Scanner**: Automated vulnerability scanner (available in Burp Professional).
- **Intruder**: Performs automated customized attacks like fuzzing, brute forcing, or parameter manipulation.
- **Repeater**: Allows manual crafting, sending, and resending of HTTP requests to test responses.
- **Sequencer**: Analyzes randomness in tokens or session IDs.
- **Decoder**: Helps encode/decode data in different formats.
- **Comparer**: Compares two pieces of data for differences.

4. How Does Spider Work in Burp Suite?

- Spider automatically **crawls** the target application by following links, forms, and URLs.
- Builds a **site map** showing all discovered pages and parameters.
- Useful to identify hidden or unlinked pages before testing.
- Spider respects robots.txt and other restrictions but can be configured to ignore them.

5. What is the Purpose of Repeater in Burp Suite?

- Repeater is a manual testing tool to **send and modify HTTP requests repeatedly**.
- Helps in fine-tuning payloads, testing input validation, and observing server responses without rescanning or re-spidering.
- Ideal for verifying suspected vulnerabilities by testing inputs and analyzing responses.

---

6. How Can Intruder Be Used for Attacks?

- Intruder automates **customized attacks** by injecting payloads into specific positions in requests.
- Common use cases:
  - Brute forcing login credentials.
  - Fuzzing parameters for SQLi, XSS, or other vulnerabilities.
  - Testing session tokens or access control bypass.
- Supports various attack types: Sniper, Battering Ram, Pitchfork, and Cluster Bomb for different payload strategies.

---

7. What is Burp Scanner and When to Use It?

- Burp Scanner is an **automated vulnerability scanner** integrated into Burp Suite Professional.
- Used to identify common security flaws like SQL injection, XSS, CSRF, and more.
- Best used after mapping the target app to cover all inputs and endpoints.
- Helps speed up assessment but should be combined with manual testing to avoid false positives/negatives.

---

8. How to Interpret Results from Burp Suite?

- Results show in tabs such as Target, Proxy history, Scanner alerts, and Intruder results.
- Vulnerabilities are usually accompanied by:
  - **Severity level** (High, Medium, Low).
  - **Detailed description** explaining the issue.
  - **Request/response samples** illustrating the flaw.
  - **Remediation advice** or references.
- Analysts must verify issues manually and assess real risk.

---

9. What Are Some Common Issues that Burp Suite Can Identify?

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

- Server misconfigurations and information leaks
- Insecure cookies and session handling
- Unvalidated redirects and forwards
- Broken authentication and authorization issues
- Sensitive data exposure

---

10. How Do You Configure Burp Suite for HTTPS Traffic?

- HTTPS is encrypted, so intercepting requires **installing Burp's CA certificate** in the browser:
  1. Go to **Proxy > Intercept > CA certificate** in Burp.
  2. Export the certificate and import it into your browser's trusted root certificate authorities.
  3. Set your browser proxy to Burp's listener (127.0.0.1:8080).
  4. Burp will now decrypt, intercept, and re-encrypt HTTPS traffic for inspection.
- Without this, browsers will warn about insecure connections.
